

# Kasra Ahmadi, Ph.D Candidate.

Tampa, FL, 33617 | E-mail: [ahmadi1@usf.edu](mailto:ahmadi1@usf.edu), Mobile: 8136142640 | Personal webpage: <https://kasraahmadi.github.io/>  
LinkedIn: <https://www.linkedin.com/in/kasra-ahmadi/> | GitHub: <https://github.com/KasraAhmadi> | [Google Scholar](#)

## Education

---

1. University of South Florida, Tampa; **Ph.D. in Computer Science**; Jan 2022 to May 2025; GPA: 3.93/4
2. Amirkabir University of Technology, Tehran; M.Sc. in Information Technology; Sep 2018 to Sep 2021.
3. Isfahan University of Technology, Isfahan; B.Sc. in Computer Science; Sep 2012 to Jul 2017.

## Skills

---

- **Data** AWS Glue, Airflow, Kafka, Kinesis, PowerBI, Postgres, MongoDB
- **ML** Pytorch, Pandas, Numpy, Flower, Scikit-learn, Huggingface
- **Programming** Python, C, C++, Verilog, Typescript, Node.js, Java, JavaScript, Bash, QT, QML, SQL
- **Cloud** Lambda, Step functions, S3, EC2, DynamoDB, Aurora, IAM, API Gateway, CloudFormation
- **IoT** Vitis, ARM Cortex-M4, FPGA, Stm32, Raspberry Pi, AVR, Arduino
- **Others** Linux, Git, Docker, Jira, GraphQL, Rest API, Wireshark, Selenium, Postman, Webservice

## Work Experience

---

- **University of South Florida, Tampa, US** Jan 2022 - Present  
Research Assistant
  - Researching fine-tuning large language models (**LLMs**) using **Federated Learning**, while ensuring privacy preserving through the implementation of **differential privacy (DP)** at the client side.
  - Researching algorithm level error detection schemes for **Number Theoretic Transform (NTT)** utilized in **Kyber** and **Dilithium**, NIST selected **Post-Quantum Cryptography (PQC)** schemes.
  - **Researching, simulating, and implementing** algorithm-level error detection schemes for classical cryptosystems such as the Montgomery Ladder and Window method for ECSM.
  - Performance assessment of Post-Quantum Cryptography schemes on **FPGAs, ARM, and Embedded Linux**.
  - Work under National Science Foundation (NSF) Grant # [1801488](#);
  - Teaching assistant of graduated Cryptography, Operating Systems, Network Lab, and System Design Lab.
- **Transparency Wise, St.Petersburg, US** May 2024 - Aug 2024  
Software Engineer, Intern
  - Led a team of 3 software engineers and 2 designers to develop a **recommender system** for nutrient recommendations tailored to various growth stages of corn and soybeans to achieve high yield farming practices.
  - Implemented an **event-driven** architecture utilizing **Lambda functions, Step Functions, Event Bridge, SES, and API Gateway** to promote loose coupling and **scalability**. Additionally, leveraged **AWS Glue** as **ETL** tool for processing laboratory reports to support the recommender model.
- **Paar Lift, Tehran, Iran** Jan 2019 - Apr 2020  
Software Engineer
  - Analyzed optimal floor levels for elevators at specific times to reduce passenger wait times using machine learning, such as **Logistic Regression** and **KNN**. Utilized data-driven approaches to enhance elevator efficiency and passenger experience.
  - Establishing a connection between Raspberry Pi embedded boards and elevators through the CAN bus protocol for the real-time data transfer of elevators to a Linux-powered **IoT**.
  - Building **ETL** pipelines by using Apache airflow to extract, ingest, and load elevator traffic data to an **OLAP** storage.
  - Performing **Data visualization, big data analytics, and statistical modeling** on elevators traffic data.
  - We decreased hotels passengers' waiting time by 27%, equating to a time savings of 11 seconds per passenger. [Project's demo](#).

## Publications

C=Conference, J=Journal, S=In Submission

- [S.1] Ahmadi, K, et al (2025), “**An Interactive Framework for Implementing Privacy-Preserving Federated Learning: Experiments on Large Language Model.**” Manuscript submitted to *IEEE Symposium on Security and Privacy 2025*
- [J.1] Aghapour, S., Ahmadi, K., Anastasova, M, et al. (2025). “**PUF-Dilithium: Design of a PUF-Based Dilithium Architecture Benchmarked on ARM Processors.**” *ACM Trans. Embed. Comput. Syst.*, 24(2).
- [J.2] Ahmadi, K., et al. (2024). “**Efficient Error Detection Schemes for ECSM Window Method Benchmarked on FPGAs.**” *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 32(3), 592-596.
- [J.3] Ahmadi, K., et al. (2024). “**Efficient Error Detection Cryptographic Architectures Benchmarked on FPGAs for Montgomery Ladder.**” *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 32(11), 2154-2158.
- [J.4] Aghapour, S., Ahmadi, K., Anastasova, M, et al. (2024). “**PUF-Kyber: Design of a PUF-Based Kyber Architecture Benchmarked on Diverse ARM Processors.**” *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 43(12), 4453-4462.
- [C.1] Ahmadi, K. et al. (2023). “**A P2P file sharing market based on blockchain and ipfs with dispute resolution mechanism.**” In *2023 IEEE International Conference on Artificial Intelligence, Blockchain, and Internet of Things (AIBThings)* (pp. 1-5).
- [S.2] Ahmadi, K, et al (2025), “**Efficient Algorithm Level Error Detection for Number-Theoretic Transform Assessed on FPGAs and ARM**” Manuscript submitted to *ACM Trans. Embed. Comput. Syst.*
- [S.3] Ahmadi, K, et al (2025), “**Error Detection Schemes for  $\tau$ -NAF Conversion within Koblitz Curves Benchmarked on Various ARM Processors**” Manuscript submitted to *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*.
- [S.4] Aghapour, S., Ahmadi, K., Kermani, M, et al (2024) “**Efficient Fault Detection Architectures for Modular Exponentiation Targeting Cryptographic Applications Benchmarked on FPGAs**” Manuscript submitted to *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems II*.
- [S.5] Darzi, S., Ahmadi, K., Aghapouri, S, et al (2023) “**Envisioning the future of cyber security in post-quantum era: A survey on pq standardization, applications, challenges and opportunities**” Manuscript submitted to *ACM Comp Survey*.

## Certifications

- **AWS Certified Solutions Architect - Associate**, [View Certification](#) (Dec 2023)
- Deep Neural Networks with PyTorch, [View Certificate](#) (Oct 2024)
- Intro to Federated Learning, [View Certificate](#) (Oct 2024)
- Artificial Intelligence Privacy and Convenience, [View Certificate](#) (Aug 2024)
- Federated Fine-tuning of LLMs with Private Data, [View Certificate](#) (Aug 2024)
- ETL and Data Pipelines with Shell, Airflow and Kafka, [View Certificate](#) (Jan 2024)
- Divide and Conquer, Sorting and Searching, and Randomized Algorithms, [View Certificate](#) (Oct 2023)

## Projects

- **Secure Microcontrollers Remote Programmer**  
Developed and designed a QT/QML application along with a server API using Node.js to enable the programming of Microchip microcontrollers remotely while preserving the company’s hex files confidentiality.
- **GPS Car Tracker**  
Utilized STM32 and ArduinoIDE for the hardware implementation. Additionally, Node.js was employed for the server API.
- **Android Game published on Google Play**  
Designed and developed an online Trivia Android game (Footxam) by using **Java** and **Node.js**.

## Services

- Mentor at REU Site: Cryptography and Coding Theory at the University of South Florida (Summer, 2023) [NSF award: 2244488](#)
- Conducted peer review for 15 manuscripts from “Transactions on Embedded Computing Systems”, “IEEE Transactions on Circuits and Systems I: Regular Papers”, and “IEEE Transactions on Very Large Scale Integration (VLSI) Systems”.
- Speaker at Great American Teach-In (Winter, 2023)